IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANTS:	Michael A. Horwitz, Kenneth W. O'Dell, Dennis J. O'Flynn, and Carlos Devoto
SERIAL NO.:	10/817,275
FILING DATE:	April 1, 2004
TITLE:	Cross-Platform Single Sign-On Data Sharing
EXAMINER:	Martin Jeriko P. San Juan
GROUP ART UNIT:	2132
ATTY. DKT. NO.:	16010-07728

CERTIFICATE OF ELECTRONIC (EFS-WEB) TRANSMISSION

I hereby certify that this correspondence is being transmitted via the Office electronic filing system in accordance with 37 C.F.R. § 1.8(a)(i)(C) from the **Pacific Time Zone** of the United States on the local date shown below.

Dated: September 22, 2008 By: /Christopher King/
Christopher P. King, Reg. No. 60,985

COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

APPEAL BRIEF

Pursuant to the requirements of 37 C.F.R. § 41.37, please consider this document as the Appellants' Brief in the present application currently before the Board of Patent Appeals and Interferences (hereinafter "the Board").

I. REAL PARTY IN INTEREST

The real party in interest in the present application is Compuware Corporation, assignee of all rights and interests in the present application. Assignment to Compuware Corporation from the inventors, Michael Horwitz, Kenneth O'Dell, Dennis O'Flynn, and Carlos Devoto, was recorded in the United States Patent and Trademark Office on April 1, 2004, at Reel 015187, Frame 0740.

II. RELATED APPEALS AND INTERFERENCES

To the best knowledge of the Appellants and the Appellants' legal representative, there are no other appeals or interferences that will directly affect, be affected by, or have a bearing on the decision of the Board in the present appeal.

III. STATUS OF CLAIMS

Claims 1-29 are currently pending in the present application. These claims were rejected in the Final Office Action of April 21, 2008 under 35 USC § 103(a) as allegedly being unpatentable over Roberts, U.S. Patent 6,295,551, in view of Satyavolu, U.S. Patent No. 7,225,464.

The rejection of claims 1-29 is hereby appealed. The claims involved in the present appeal are recited in Section VIII.

IV. STATUS OF AMENDMENTS

All claim amendments submitted to the Examiner during prosecution of the present application have been entered. The claims involved in the present appeal are presented in

Section VIII.

V. SUMMARY OF CLAIMED SUBJECT MATTER

In general, embodiments of the claimed invention involve the use of authentication and non-authentication data with a plurality of independent local applications.

1. Independent Claim 1

Independent claim 1 is directed to a cross-platform single sign-on system for sharing user data across computers on a plurality of computing platforms, the system comprising:

(i) an authentication module for authenticating a user at the beginning of a computing session (*See, e.g.,* Specification, paragraph 0032);

(ii) an interface module configured to receive requests for authentication and non-authentication data associated with the user from a plurality of independent local applications on the plurality of computing platforms (*See, e.g.,* Specification, paragraphs 0015, 0047, 0054, and 0058, and Figures 1 and 4) and, based upon authentication of the user at the beginning of the computing session and responsive to the requests, to automatically provide authentication and non-authentication data to the plurality of independent local applications throughout the computing session (*See, e.g.*, paragraphs 0017 and 0051, and Figure 3); and

(iii) a data registry in communication with the interface module for storing and providing authentication data and non-authentication data responsive to

requests made by the plurality of independent local applications (*See, e.g.,* Specification, paragraph 0015 and Figure 4).

2. Independent Claim 14

Independent claim 14 is directed to a data registry for storing and providing data across a computing system, the data registry comprising:

(i) a plurality of user data entries, each of the user data entries describing a unique user of a computing system comprised of a plurality of computing platforms and a plurality of independent local applications (*See, e.g.,* Specification, paragraph 0015);

(ii) a plurality of authentication entries associated with each of the user data entries for authenticating the user on the plurality of independent local applications of the computing system (*See, e.g.,* Specification, paragraph 0015); and

(iii) a plurality of non-authentication attributes and attribute entries associated with each of the user data entries in which information about a user's use of a local application can be preserved (*See, e.g.,* Specification, paragraph 0015).

3. Independent Claim 18

Independent claim 18 is directed to a method of sharing data across a computing system, the method comprising:

(i) subsequent to an initial authentication of a user, receiving requests to authenticate the authenticated user from a plurality of independent local applications on a plurality of computing platforms being accessed by the authenticated user (*See, e.g.,* Specification, paragraphs 0015, 0047, and 0032, and Figure 3);

(ii) automatically authenticating the authenticated user to the plurality of independent local applications being accessed by the authenticated user responsive to the initial authentication of the user (*See, e.g.,* Specification, Figure 3);

(iii) receiving non-authentication data provided by a first instance of the authenticated user using a local application in a first domain (*See, e.g.,* Specification, paragraph 0023);

(iv) storing in a data registry the non-authentication data provided by the first instance of the authenticated user using the local application in the first domain (*See, e.g.,* Specification, paragraph 0023);

(v) receiving a request for non-authentication data from a second instance of the local application in a second domain (*See, e.g.,* Specification, paragraph 0034); and

(vi) supplying, from the data registry, the requested non-authentication data provided by the first instance of the local application in the first domain to the second instance of the local application in the second domain (*See, e.g.,* Specification, paragraph 0034).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The ground of rejection presented for review in the present appeal is as follows:

1. Whether the combination of Roberts and Satyavolu renders claims 1-29 unpatentable under 35 U.S.C. § 103(a).

VII. ARGUMENT

A. Claims 1-29 are Patentable over Roberts and Satyavolu

To establish a *prima facie* case of obviousness, the prior art reference (or references when combined) must suggest or teach *all* the limitations of the claimed invention. *See In re Royka*, 490 F.2d 981 (C.C.P.A. 1974); 35 U.S.C. § 103(a); MPEP §§ 706.02(j), 2143.03. If even a single claim limitation is not taught or suggested by the prior art, then that claim cannot be obvious over the prior art. *See In re Glass*, 472 F.2d 1388, 1392 (C.C.P.A. 1973).

Independent claim 1 recites a cross-platform single sign-on system for sharing user data across computers on a plurality of computing platforms, the system comprising, in part:

> ...
> an interface module configured to receive **requests** for authentication and non-authentication data associated with the user **from a plurality of independent local applications** on the plurality of computing platforms and, based upon authentication of the user at the beginning of the computing session and responsive to the requests, to automatically provide authentication and non-authentication data to the plurality of independent local applications throughout the computing session; and
> a data registry in communication with the interface module for storing and providing authentication data and non-authentication data **responsive to requests made by the plurality of independent local applications**.
> ...

Thus, the claimed interface module is configured to receive requests from a plurality of **independent local** applications.

In past Office Actions, the Examiner cited Roberts as allegedly disclosing this feature. Roberts discusses a call center system enabling a call center representative and a calling party to jointly browse World Wide Web content while simultaneously conducting a voice conversation. (Roberts, Abstract). After a user provides a password, the server provides an applet enabling the joint activities (Roberts 11:5-44). Specifically, the server provides a user applet to the calling party's computer and a service applet to the call center representative's computer (Roberts Abstract). The applets then can proceed to share data (16:9-39), such as a demonstration or form.

As Applicants previously established in the Response of January 24, 2008, the applets of Roberts are not "independent local applications." As explained in the Response, applets are downloaded and run in response to the decision of a server and are thus plainly not "local," and they exist solely for the purpose of communicating with the other downloaded applet and thus are not "independent." The Examiner, presumably agreeing with Applicants, then alleged in the

Office Action of April 21, 2008, that it is the **browser** applications of Roberts that constitute the claimed "independent local applications." (Office Action of April 21st, page 3).

However, this alternate interpretation is likewise deficient. The browsers of Roberts merely act as host execution environments in which the user applets and service applets execute and perform their operations. Note that an applet does not even require a browser to execute, but can execute in a stand-alone environment such as Sun's AppletViewer or other process capable of interpreting the applet code, and thus any link between the browsers and the applets is merely incidental. It is the applets—i.e. the user applet and service applet downloaded from a server—that control the transmission of user view information with each other. Without the applets, the browsers standing alone would not transmit any information between themselves. Thus, any requests for authentication and non-authentication data that could be said to occur in Roberts are properly deemed to be performed by the applets, not by the browser environments in which the applets execute.

Further, as has already been established, applets in no way constitute "independent local applications." The Examiner notes on page 3 of the Office Action of April 21st that FIG. 2B and paragraph 0041 of Applicants' specification show a browser application. However, this merely shows that an application (specifically, Optimal View) can be run from within a web browser, a point which is not in dispute and which in any case does not support the Examiner's interpretation. Merely because the application can be run within a web browser does not make **the web browser** itself an "independent local application" that makes requests "for authentication and non-authentication data associated with the user," as claimed. Rather, as noted above with respect to applets, the web browser is merely an execution environment in which an application executes, and does not itself make requests for authentication and non-

authentication data. Thus, Roberts fails to disclose or suggest that the requests for authentication and non-authentication data are made by "a plurality of independent local applications."

Nor does Satyavolu remedy the deficiencies of Roberts. Satyavolu discloses a network-based software application enabling a user to log-in to multiple password-protected web sites using only one manual authentication. (Satyavolu Abstract, 1:66-2:3; 3:56-60). However, remote web pages are clearly not "local applications," as is claimed, nor does the Examiner assert that they are. Thus, the combination of Roberts and Satyavolu does not render the claimed invention obvious, and a person of ordinary skill in the art considering the teachings of the references would not have found claim 1 to be obvious at the time the invention was made.

Independent claims 14 and 18, like independent claim 1, recite "independent local applications," and are thus patentable over Roberts and Satyavolu for the same reasons discussed above with respect to claim 1.

Nor do Roberts and Satyavolu disclose or suggest the additional features recited in dependent claims 12 and 16. For example, claim 12 recites "a caching module for storing non-authentication data generated by an application in the local cache of the computer hosting the local application ***when the computer is disconnected from the computing system***." The Examiner cited Roberts 9:25-38, which states that the user applet is "persistent," and will "remain disposed on the user computer 12 such that it will not have to be downloaded again from the server." Although Applicants, like the Examiner, had previously made the assumption that a "persistent" applet would remain across sessions, a closer inspection of the overall context of the paragraph reveals that this persistence is in fact limited to the current session and does not remain across sessions. For example, 9:29-31 states that "the user applet 22 remains on the user computer 12 as long as the user computer 12 ***remains in the session with the server***," thus

showing that remaining in the session is a prerequisite to the applet's persistence. The final sentence of the paragraph, 9:36-38, notes that in this way, the user applet will remain in the cache regardless of any changes to the user interface of the user computer. Such changes to the user interface, such as the display of a new page in which the user applet is embedded, would of course occur during browsing within the same session, not outside the session. Since a session with the server would naturally end when a computer is disconnected from the network, Roberts thus cannot show the claimed "storing non-authentication data… when the computer is disconnected from the system."

Claim 16 recites that the non-authentication data of claim 14 includes configuration information for one of the plurality of independent local applications. The Examiner cited Roberts 12:66-13:60, which discloses the use of scripts, code providing a mechanism for controlling what information is displayed within a browser. (Roberts 12:66-67). However, dependent claim 16 must be read in the context of its parent claim 14, which recites that non-authentication attributes and attribute entries are comprised by the data registry, are associated with user data entries describing a unique user of the computing system, and preserve information about a user's use of the application. In contrast, Roberts does not disclose that the scripts are comprised by a data registry, are associated with user data entries, or *preserve* information about use of an application (as opposed to merely controlling it at runtime).

Thus, the cited references likewise fail to disclose the additional features of claims 12 and 16 for at least these additional reasons. The remaining claims all depend, directly or indirectly, from one of independent claims 1, 14, and 18, and are thus patentably distinguishable over the cited references for at least the same reasons discussed above with respect to their respective independent claims.

B. Conclusion

The arguments presented herein demonstrate that claims 1-29 of the present application are patentable over the prior art of record. Therefore, Appellants respectfully request that the Board reverse the Examiner's rejections of these claims.

Respectfully Submitted,
MICHAEL A. HORWITZ ET AL.

Date: September 22, 2008

By: /Christopher King/

Christopher P. King, Reg. No. 60,985
FENWICK & WEST LLP
801 California Street
Mountain View, CA 94041
Phone: (650) 335-7633
Facsimile: (650) 938-5200

VIII. CLAIMS APPENDIX

The claims involved in the present appeal are as follows:

1. A cross-platform single sign-on system for sharing user data across computers on a plurality of computing platforms, the system comprising:

an authentication module for authenticating a user at the beginning of a computing session;

an interface module configured to receive requests for authentication and non-authentication data associated with the user from a plurality of independent local applications on the plurality of computing platforms and, based upon authentication of the user at the beginning of the computing session and responsive to the requests, to automatically provide authentication and non-authentication data to the plurality of independent local applications throughout the computing session; and

a data registry in communication with the interface module for storing and providing authentication data and non-authentication data responsive to requests made by the plurality of independent local applications.

2. The cross-platform single sign-on system of claim 1, wherein web services technologies are used to transmit requests for authentication and non-authentication data from a plurality of computer systems hosting the plurality of applications to the interface module.

3. The cross-platform single sign-on system of claim 1, wherein the non-authentication data includes state information reflecting a state of a selected local application on a first computer

accessed by the user that can be retrieved when the selected local application is being accessed from a second computer.

4. The cross-platform single sign-on system of claim 3, wherein the selected local application is being accessed from a second computer by a second user.

5. The cross-platform single sign-on system of claim 1, wherein the interface module is further configured to receive requests to store authentication and non-authentication data associated with the user from a plurality of independent local applications on a plurality of computing platforms in the computing system and, based upon authentication of a user at the beginning of a computing session and responsive to the requests, to store the data to the data registry.

6. The cross-platform single sign-on system of claim 1, wherein the interface module formats data queries to the data registry in accordance with a data exchange protocol accepted by the data registry.

7. The cross-platform single sign-on system of claim 1, wherein the data registry is further configured to receive requests for authentication and non-authentication data directly from the plurality of independent local applications on the plurality of computing platforms, and for the requested data to be retrieved from the data registry responsive to the requests.

8. The cross-platform single sign-on system of claim 1, wherein a request to retrieve authentication and non-authentication data associated with the user is sent responsive to an event trigger activated during the user's computing session.

9. The cross-platform single sign-on system of claim 8, wherein the event trigger comprises at least one of: the authentication of a user, a user command, and the passage of a pre-determined interval of time.

10. The cross-platform single sign-on system of claim 1, wherein the interface module and authentication module are commonly hosted on a single computer.

11. The cross-platform single sign-on system of claim 1, wherein at least one of the plurality of computing platforms differs from at least another of the plurality of computing platforms.

12. The cross-platform single sign-on system of claim 1, further comprising:

a caching module for storing non-authentication data generated by an application in the local cache of the computer hosting the local application when the computer is disconnected from the computing system; and

a synchronizing module for sending non-authentication data stored in the local cache to the data registry when the computer is connected to the computing system.

13. The cross-platform single sign-on system of claim 1, wherein the authentication module is configured to detect that a user is logging on to the system for the first time, further comprising:

a verification module in communication with the data registry for verifying the identity of the user;

a password capture utility launched responsive to the successful verification of the user's identity for creating a global user id and password for the user with which the user can be logged on to the cross-platform single sign-on system, capturing user authentication information associated with applications launched during the user's computing session, and storing the authentication information in the data registry.

14. A data registry for storing and providing data across a computing system, the data registry comprising:

a plurality of user data entries, each of the user data entries describing a unique user of a computing system comprised of a plurality of computing platforms and a plurality of independent local applications;

a plurality of authentication entries associated with each of the user data entries for authenticating the user on the plurality of independent local applications of the computing system; and

a plurality of non-authentication attributes and attribute entries associated with each of the user data entries in which information about a user's use of a local application can be preserved.

15. The data registry of claim 14, wherein the non-authentication data includes state information for one of the plurality of independent local applications, whereby a user may switch between a first computer and a second computer and preserve the state of a selected application accessed using the first computer when accessing the selected application from the second computer.

16. The data registry of claim 14, wherein the non-authentication data includes configuration information for one of the plurality of independent local applications with which a user's application environment can be customized.

17. The data registry of claim 14, further comprising an interface module that receives web service requests for storing and providing data from one of the plurality of independent local applications and, responsive to the requests, saves the data to the data registry.

18. A method of sharing data across a computing system, the method comprising:

subsequent to an initial authentication of a user, receiving requests to authenticate the authenticated user from a plurality of independent local applications on a plurality of computing platforms being accessed by the authenticated user;

automatically authenticating the authenticated user to the plurality of independent local applications being accessed by the authenticated user responsive to the initial authentication of the user;

receiving non-authentication data provided by a first instance of the authenticated user using a local application in a first domain;

storing in a data registry the non-authentication data provided by the first instance of the authenticated user using the local application in the first domain;

receiving a request for non-authentication data from a second instance of the local application in a second domain; and

supplying, from the data registry, the requested non-authentication data provided by the first instance of the local application in the first domain to the second instance of the local application in the second domain.

19. The method of claim 18, wherein the second instance of the local application in the second domain is associated with a second user.

20. The method of claim 18, further comprising:

receiving log on information from a user;

determining that the user is logging on to the computing system for the first time;

subsequent to the determination that a user is logging on to the computing system for the first time, verifying the identity of the user;

prompting the user to supply a user id and password;

providing the user id and password supplied by the user to a data registry to be stored therein;

capturing application authentication information provided by the user during the computing session;

storing the application authentication information provided by the user during the computing session in the data registry wherein the data registry is configured to store authentication and non-authentication data.

21. The method of claim 18, wherein an operating platform used by the first domain differs from an operating platform used by the second domain.

22. The method of claim 18, further comprising storing authentication data in the data registry.

23. The method of claim 18, wherein the non-authentication data provided by the first instance of the application in the first domain comprises configuration information for customizing a user's application environment.

24. The method of claim 18, wherein the non-authentication data provided by the first instance of the local application in the first domain includes state information with which the user's application state from the first instance of the local application in the first domain can be maintained to the second instance of the local application in the second domain.

25. The method of claim 18, wherein storing the non-authentication data comprises:

configuring a non-authentication data attribute;

storing a value for the non-authentication data attribute associated with the user; and

responsive to a request identifying the non-authentication data attribute, providing the value of the non-authentication data attribute to a requesting application.

26. The method of claim 18, wherein the request for non-authentication data associated with the authenticated user is generated responsive to a call trigger.

27. The method of claim 18, wherein the step of receiving non-authentication data provided by a first instance of an application used by the authenticated user comprises receiving the non-authentication data from a synchronizing module on a computer for sending non-authentication data from the local cache of the computer, the data having been stored in the local cache when the authenticated user was disconnected from the networked system.

28. The system of claim 1, wherein the non-authentication data comprises one of: configurations data, settings data, or applications data, environment data.

29. The system of claim 1, wherein the non-authentication data comprises one of: a size of a window, the configuration of a tool bar, and the selection of open files.

IX. EVIDENCE APPENDIX

No evidence of the types described in 37 CFR § 41.37(c)(1)(ix) has been submitted during prosecution of the present application.

X. RELATED PROCEEDINGS APPENDIX

As indicated in Section II, to the best knowledge of the Appellants and the Appellants' legal representative, there are no decisions rendered by a court or the Board that may directly affect, be affected by, or have a bearing on the decision of the Board in the present appeal.